UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

ZACHARY LOAFMAN, on behalf of himself and all others similarly situated, Plaintiff, v. **BELLE TIRE DISTRIBUTORS, INC.,** Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Zachary Loafman ("Plaintiff"), individually and on behalf of all similarly situated persons, allege the following against Belle Tire Distributors, Inc. ("Belle Tire" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Belle Tire for its failure to properly secure and safeguard Plaintiff's and other similarly situated current and former employees' ("Class Members") personally identifiable information ("PII") from hackers.

2. Belle Tire, based in Southfield, Michigan, is an automotive services company that serves thousands of customers in multiple states.

3. On or about October 31, 2024, Belle Tire filed official notice of a hacking incident with the Office of the Maine Attorney General.

4. On or about the same time, Belle Tire also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice, Belle Tire detected unusual activity on some of its computer systems on June 11, 2024. In response, the company conducted an investigation which revealed that an unauthorized party had access to certain company files on or around the same date (the "Data Breach"). Yet, Belle Tire waited more than 3 months to notify the public that they were at risk.

6. As a result of this delayed response, Plaintiff and "Class Members" (defined below) had no idea for more than 3 months that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, current and former employees' name, address, date of birth, Social

Security number, and driver's license number that Belle Tire collected and maintained.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by Belle Tire that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

10. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiff brings this class action lawsuit to address Belle Tire's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiff and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Belle Tire, and thus Belle Tire was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, Belle Tire and its employees failed to properly monitor or implement security practices with regard to the computer network and systems that housed the Private Information. Had Belle Tire properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiff's and Class Members' identities are now at risk because of Belle Tire's negligent conduct as the Private Information that Belle Tire collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for negligence, invasion of privacy, breach of implied contract, unjust enrichment, and declaratory judgment.

II. PARTIES

17. Plaintiff Zachary Loafman is an individual citizen of the State of Michigan.

18. Defendant Belle Tire is an automotive service provider with its principal place of business at 25800 Northwestern Highway, Southfield Michigan, 48075.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Belle Tire. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over Belle Tire because Belle Tire is incorporated and conducts business in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Belle Tire resides in this District and is being served in this District.

IV. FACTUAL ALLEGATIONS

A. Belle Tire's Business and Collection of Plaintiff's and Class Members' Private Information

22. Founded in 1922, Belle Tire is an American tire, wheel and automotive service retailer providing tire repair, alignment, brakes, and other mechanical services.[1] Belle Tire operates more than 175 locations in Michigan, Indiana, Ohio and Illinois.[2] Belle employs approximately 3,000 individuals and generates approximately $350 million in annual revenue.[3]

23. As a condition of employment with Belle Tire, Defendant requires that its employees entrust it with highly sensitive personal information. In the ordinary course of employment with Belle Tire, Plaintiff and Class Members were required to provide their Private Information to Defendant.

24. Because of the highly sensitive and personal nature of the information Belle Tire acquires and stores with respect to its employees, Belle Tire, upon information and belief, promises to, among other things: keep employees' Private Information private; comply with industry standards related to data security and the maintenance of its employees' Private Information; inform its employees of its legal duties relating to data security and comply with all federal and state laws protecting

[1] *See* https://www.linkedin.com/company/belle-tire (last visited Nov. 12, 2024).
[2] *Id.*
[3] *Id.*

employees' Private Information; only use and release employees' Private Information for reasons that relate to the services it provides; not store former employees' Private Information for longer than is necessary to carry out its business operations; and provide adequate notice to its current and former employees if their Private Information is disclosed without authorization.

25. By obtaining, collecting, using, and deriving a benefit from its employees' Private Information, Belle Tire assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

26. Plaintiff and Class Members relied on Belle Tire to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Defendant's Inadequate Notice to Plaintiff and Class Members

27. In a data breach notice letter that went out to all impacted current and former Belle Tire employees on or around October 31, 2024 (the "Notice"), Defendant reported that it learned of unauthorized access to its computer systems approximately 3 months earlier on or around June 11, 2024. Based upon the company's investigation, it discovered that the Data Breach was the result of an attack on its systems that allowed an "cybercriminal" to gain access to its systems and ultimately access copies of Plaintiff's and Class Members' Private Information.

It is clear that the data thieves carried out this attack in order to either use the Private Information themselves for nefarious purposes, or to sell it on the dark web.

28. According to Defendant's Notice, it learned of unauthorized access to its computer systems on June 11, 2024, with such unauthorized access having taken place on or around the same date.

29. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including customers' name, address, date of birth, Social Security number, and driver's license number, of at least 29,330 of individuals.

30. On or about October 31, 2024, roughly 3 months after Belle Tire learned that the Class's Private Information was first accessed by cybercriminals, Belle Tire finally began to notify customers that its investigation determined that their Private Information was "seen and taken".

31. Belle Tire delivered Data Breach Notification Letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "incident."

32. Omitted from the Notice are crucial details like the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been

explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

33. Thus, Belle Tire's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiff and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

34. In addition, the Notice offers no substantive steps to help victims like Plaintiff and Class Members to protect themselves other than providing two years of credit monitoring – an offer that is woefully inadequate considering the lifelong increased risk of fraud and identity theft Plaintiff and Class Members now face as a result of the Data Breach.

35. Belle Tire had obligations created by contract, industry standards, and common law to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

36. Plaintiff and Class Members provided their Private Information to Belle Tire with the reasonable expectation and mutual understanding that Belle Tire would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

37. Belle Tire's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

38. Belle Tire knew or should have known that its electronic records would be targeted by cybercriminals.

C. Belle Tire Knew or Should Have Known of the Risk of a Cyber Attack Because Businesses in Possession of Private Information are Particularly Suspectable.

39. Belle Tire's negligence, including its gross negligence, in failing to safeguard Plaintiff's and Class Members' Private Information is particularly stark, considering the highly public increase of cybercrime, like the hacking incident that resulted in the Data Breach.

40. Data thieves regularly target entities that store PII like Belle Tire due to the highly sensitive information they maintain. Belle Tire knew and understood that Plaintiff's and Class Members' Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize it through unauthorized access.

41. According to the Identity Theft Resource Center's 2023 Data Breach Report, the overall number of publicly reported data compromises in 2023 increased more than 72-percent over the previous high-water mark and 78-percent over 2022,

impacting an estimated 353,027,892 individuals."[4]

42. Despite the prevalence of public announcements of data breach and data security compromises, Belle Tire failed to take appropriate steps to protect Plaintiff's and Class Members' Private Information from being compromised in this Data Breach.

43. As a national service provider in possession of millions of employees' Private Information, Belle Tire knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class Members and of the foreseeable consequences they would suffer if Belle Tire's data security systems were breached. Such consequences include the significant costs imposed on Plaintiff and Class Members due to the unauthorized exposure of their Private Information to criminal actors. Nevertheless, Belle Tire failed to take adequate cybersecurity measures to prevent the Data Breach or the foreseeable injuries it caused.

44. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals, for use in variety of different injurious ways. Indeed,

[4] *2023 Annual Data Breach Report*, IDENTITY THEFT RESOURCE CENTER, (Jan. 2024), *available online at*: https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf (last visited on Nov. 12, 2024).

the cybercriminals who possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

45. Belle Tire was, or should have been, fully aware of the unique type and the significant volume of data on Belle Tire's network server(s) and systems, amounting to thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

46. Plaintiff and Class Members were the foreseeable and probable victims of Belle Tire's inadequate security practices and procedures. Belle Tire knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that data, particularly due to the highly public trend of data breach incidents in recent years.

D. Belle Tire Failed to Comply with FTC Guidelines

47. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of

Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

48. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[5] The guidelines note that businesses should protect the personal information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

49. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for

[5] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (October 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on Nov. 12, 2024).

suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

50. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect Personal Information by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 *et seq*. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

51. Such FTC enforcement actions include those against businesses that fail to adequately protect Personal Information, like Belle Tire here. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

52. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Belle Tire of failing to use reasonable measures to protect Private Information they collect and maintain from consumers. The FTC publications and orders described above also form part of the basis of Belle Tire's duty in this regard.

53. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[6]

54. As evidenced by the Data Breach, Belle Tire failed to properly implement basic data security practices. Belle Tire's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

55. Belle Tire was at all times fully aware of its obligation to protect the Private Information of its employees, yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[6] FTC Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), *transcript available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on Nov. 12, 2024).

E. Belle Tire Failed to Comply with Industry Standards

56. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

57. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[7]

58. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.
b. Use security software to protect data.
c. Encrypt sensitive data, at rest and in transit.

[7] *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited on Nov. 12, 2024).

d. Conduct regular backups of data.
e. Update security software regularly, automating those updates if possible.
f. Have formal policies for safely disposing of electronic files and old devices.
g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

59. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the

organization is prepared to respond if an intrusion occurs," and other steps.[8]

60. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

F. Belle Tire Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

61. In addition to its obligations under federal and state laws, Belle Tire owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Belle Tire owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and

[8] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited Nov. 12, 2024).

requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of its current and former employees.

62. Belle Tire breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Belle Tire's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect current and former employees' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

e. Failing to adhere to industry standards for cybersecurity as discussed above; and

f. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

63. Belle Tire negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer

network and systems which contained unsecured and unencrypted Private Information and exfiltrate such Private Information.

64. Had Belle Tire remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

65. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft.

G. As a result of the Data Breach, Plaintiff's and Class Members Are at a Significantly Increased Risk of Fraud and Identity Theft.

66. The FTC hosted a workshop to discuss "informational injuries," which are injuries that current and former employees like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[9] Exposure of highly sensitive personal information that

[9] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* FEDERAL TRADE COMMISSION, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Nov. 12, 2024).

individuals to keep private may cause harm to them, such as the ability to obtain or keep employment. Individuals' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

67. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

68. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

69. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

70. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

71. One such example of how malicious actors may compile Private Information is through the development of "Fullz" packages.

72. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

73. The development of "Fullz" packages means that the stolen Private

Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

74. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[10] However, these steps do not guarantee protection

[10] *See IdentityTheft.gov,* FEDERAL TRADE COMMISSION, *available at*: https://www.identitytheft.gov/Steps (last visited on Nov. 12, 2024).

from identity theft but can only mitigate identity theft's long-lasting negative impacts. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big ***data*** in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

75. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[11] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

76. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark

[11] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. DEP'T OF JUSTICE (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited on Nov. 12, 2024).

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019), *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited on Nov. 12, 2024).

web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[13]

77. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming affected individuals, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[14]

78. The Dark Web Price Index of 2023, published by PrivacyAffairs[15] shows how valuable just email addresses alone can be, even when not associated with a financial account:

---

[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web (last visited on Nov. 12, 2024).

[14] *See Dark Web Price Index: The Cost of Email Data,* MAGICSPAM, https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Nov. 12, 2024).

[15] *See Dark Web Price Index 2023*, PRIVACY AFFAIRS, https://www.privacyaffairs.com/dark-web-price-index-2023/ (last visited on Nov. 12, 2024).

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

79. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

80. Likewise, the value of PII is increasingly evident in our digital economy. Many companies, including Belle Tire, collect PII for purposes of data analytics and marketing. These companies collect PII to better target customers, and share it with third parties for similar purposes.[16]

81. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[17]

[16] *See Privacy Policy*, ROBINHOOD, https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Nov. 12, 2024).

[17] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

82. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

83. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

84. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs their ability to participate in the economic marketplace.

85. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of PII in its 2023 Consumer Impact Report.[18] After

[18] *2023 Consumer Impact Report* (Jan. 2024), IDENTITY THEFT RESOURCE CENTER, *available online at*: https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf (last visited on Nov. 12, 2024).

interviewing over 14,000 identity crime victims, researchers found that as a result of the criminal misuse of their PII:

- 77-percent experienced financial-related problems;
- 29-percent experienced financial losses exceeding $10,000;
- 40-percent were unable to pay bills;
- 28-percent were turned down for credit or loans;
- 37-percent became indebted;
- 87-percent experienced feelings of anxiety;
- 67-percent experienced difficulty sleeping; and
- 51-percent suffered from panic of anxiety attacks.[19]

86. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[20]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

[19] *Id.* at pp 21-25.

[20] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited on Nov. 12, 2024).

87. PII is a valuable commodity to identity thieves because once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

88. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future and have no choice but to vigilantly monitor their accounts and purchase credit monitoring and identity theft protection for many years to come.

H. Plaintiff's and Class Members' Experience and Resulting Damages

Plaintiff Zachary Loafman's Experience

89. Plaintiff Loafman is a former employee of Defendant. As a condition of employment with Defendant, Plaintiff Loafman was required to give his Private Information to Defendant.

90. On or about October 31, 2024, Plaintiff Loafman received the Notice, which told him that his Private Information had been "seen and taken" during the Data Breach. *See* **Exhibit A**. The Notice informed him that the Private Information compromised included his name, address, date of birth, Social Security number, and driver's license number. *Id.*

91. The Notice offered Plaintiff Loafman only two years of credit monitoring services. *Id.* Two years of credit monitoring is not sufficient given that

Plaintiff Loafman will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of his Private Information.

92. Plaintiff Loafman suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

93. Plaintiff Loafman would not have provided his Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its employees' personal information from theft, and that those systems were subject to a data breach.

94. Plaintiff Loafman suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Breach.

95. Plaintiff Loafman suffered actual injury in the form of damages to and diminution in the value of his personal information – a form of intangible property that Plaintiff Loafman entrusted to Defendant for the purpose of receiving automotive services from Defendant and which was compromised in, and as a result of, the Data Breach.

96. Plaintiff Loafman suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

97. Plaintiff Loafman has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Belle Tire fails to undertake the necessary and appropriate security and training measures to protect its employees' Private Information

98. As a result of the Data Breach, Plaintiff Loafman made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options he will now need to use. Plaintiff Loafman has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

99. As a result of the Data Breach, Plaintiff Loafman has suffered anxiety as a result of the release of his Private Information to cybercriminals, which Private Information he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of committing cyber and other crimes against him. Plaintiff Loafman is very concerned about this increased,

substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on his life.

100. Plaintiff Loafman also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Loafman; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

101. As a result of the Data Breach, Plaintiff Loafman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

102. In sum, Plaintiff and Class Members are at an imminent, immediate, and continuing increased risk of experiencing devastating instances of identity theft, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, unauthorized charges made on their financial accounts, and other forms of identity theft.

103. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such

Private Information to continue to carry out such targeted schemes against Plaintiff and Class Members.

104. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which has been and will continue to be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

105. Further, as a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach. Specifically, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

106. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

107. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach.

Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[21] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[22]

108. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

---

[21] *See How Data Brokers Profit from the Data We Create*, THE QUANTUM RECORD, https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/ (last visited on Nov. 12, 2024).

[22] *Frequently Asked Questions,* NIELSEN COMPUTER & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on Nov. 12, 2024).

109. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

110. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Belle Tire, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

111. As a direct and proximate result of Belle Tire's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

112. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

113. Specifically, Plaintiff proposes the following Nationwide Class (referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> **All individuals in the United States whose Private Information was accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.**

114. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

115. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class as well as to add subclasses, before the Court determines whether certification is appropriate.

116. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

117. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of at least 29,330 current and former employees of Belle Tire whose data was compromised in the Data Breach. The identities of Class Members are

ascertainable through Belle Tire's records, Class Members' records, publication notice, self-identification, and other means.

118. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Belle Tire engaged in the conduct alleged herein;

b. When Belle Tire learned of the Data Breach;

c. Whether Belle Tire's response to the Data Breach was adequate;

d. Whether Belle Tire unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

e. Whether Belle Tire failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether Belle Tire's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Belle Tire's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Belle Tire owed a duty to Class Members to safeguard their Private Information;

i. Whether Belle Tire breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers exfiltrated Class Members' Private Information via the Data Breach;

k. Whether Belle Tire had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

l. Whether Belle Tire breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether Belle Tire knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiff and Class Members suffered as a result of Belle Tire's misconduct;

o. Whether Belle Tire's conduct was negligent;

p. Whether Belle Tire was unjustly enriched;

q. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

r. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

119. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

120. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

121. Predominance. Belle Tire has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Belle Tire's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

122. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of

common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Belle Tire. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

123. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Belle Tire has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

124. Finally, all members of the proposed Class are readily ascertainable. Belle Tire has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Belle Tire.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

125. Plaintiff restates and realleges allegations stated from the preceding paragraphs as if fully set forth herein.

126. Belle Tire knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

127. Belle Tire knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Belle Tire was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

128. Belle Tire owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Belle Tire's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect current and former employees' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA and applicable industry standards;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To precisely disclose the type(s) of information compromised.

129. Belle Tire's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

130. Belle Tire's duty also arose because Defendant was bound by industry standards to protect its current and former employees' confidential Private Information.

131. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Belle Tire owed them a duty of care not to subject them to an unreasonable risk of harm.

132. Belle Tire, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within its possession.

133. Belle Tire, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

134. Belle Tire breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to comply with the FTCA and applicable industry standards;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

135. Belle Tire had a special relationship with its current and former employees, including Plaintiff and Class Members.

136. Plaintiff's and Class Members' willingness to entrust Belle Tire with their Private Information was predicated on the understanding that Belle Tire would take adequate security precautions to protect it. Moreover, only Belle Tire had the ability to protect its systems (and the Private Information stored thereon) from attack.

137. Belle Tire's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated, as alleged herein and admitted by Defendant in its Notice to Plaintiff and Class Members.

138. Belle Tire's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

139. As a result of Belle Tire's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of criminal third parties, has been and will continue to be used for fraudulent purposes.

140. Belle Tire also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information.

141. As a direct and proximate result of Belle Tire's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

142. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

143. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

144. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Belle Tire to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
INVASION OF PRIVACY
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

145. Plaintiff restates and realleges allegations stated from the preceding paragraphs as if fully set forth herein.

146. Plaintiff and Class Members maintain a privacy interest in their Private Information, which is highly sensitive, confidential information that is also protected from disclosure by applicable laws and industry standards, as set forth above.

147. Plaintiff's and Class Members' Private Information was contained, stored, and managed electronically in Defendant's records, computers, and databases and was intended to be secured from unauthorized access to third-parties because highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities were only shared with Defendant for the limited purpose of obtaining employment.

148. Additionally, Plaintiff's and Class Members' Private Information is highly attractive to criminals who can nefariously use such Private Information for fraud, identity theft, and other crimes without the victims' knowledge and consent.

149. Defendant's disclosure of Plaintiff's and Class Members' Private Information to unauthorized third parties by allowing such parties to gain access to its network resulted from Defendant's failure to adequately secure and safeguard Plaintiff's and Class Members' Private Information. Such failure was the direct and

proximate cause of unauthorized intrusions into Plaintiff's and Class Members' places of solitude and seclusion that are highly offensive to a reasonable person.

150. Such exploitation of Plaintiff's and Class Members' Private Information was done for Defendant's business purposes.

151. Belle Tire's unauthorized disclosure of Plaintiff's and Class Members' Private Information to criminal third parties permitted the electronic intrusion into private quarters where Plaintiff's and Class Members' Private Information was stored.

152. Plaintiff and Class Members have been damaged by Belle Tire's conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT III
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

153. Plaintiff restates and realleges allegations stated from the preceding paragraphs as if fully set forth herein.

154. Belle Tire provided employment to Plaintiff and Class Members.

155. Defendant, as employer, held the Private Information on behalf of Plaintiff and Class Members. Holding Plaintiff and Class Members' Private Information was part of Defendant's regular business practices, as agreed by the

parties. When Plaintiff and Class Members joined Defendant's employment, they agreed to have their Private Information stored in Defendant's network.

156. Plaintiff and Class Members entered implied contracts with Defendant in which Defendant agreed to safeguard and protect such Information and to timely detect any breaches of their Private Information. Plaintiff and Class Members were required to share Private Information to obtain employment. In entering such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

157. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendant.

158. Defendant's implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6)

implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

159. Defendant breached these implied promises it made with Plaintiff and Class Members by failing to safeguard and protect their Private Information and by failing to notify Plaintiff and Class Members thereof within a reasonable time.

160. Plaintiff and Class Members would not have entrusted their Private Information to Belle Tire in the absence of such an implied contract.

161. Had Belle Tire disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices in place to secure such sensitive data, Plaintiff and Class Members would not have provided their Private Information to Belle Tire.

162. Belle Tire recognized that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiff and the other Class Members.

163. Belle Tire violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information.

164. Plaintiff and Class Members have been damaged by Belle Tire's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

165. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free lifetime credit monitoring to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

166. Plaintiff restates and realleges allegations stated from the preceding paragraphs as if fully set forth herein.

167. This Count is pleaded in the alternative to Count III above.

168. Plaintiff and Class Members conferred a benefit on Defendant. Specifically, they provided Defendant with their Private Information, which Private Information has inherent value. In exchange, Plaintiff and Class Members should have been entitled to have Defendant protect their Private Information with adequate data security, especially in light of their employer-employee relationship.

169. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the

Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff and Class Members' Private Information for business purposes.

170. Defendant failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

171. Defendant acquired the Private Information through inequitable record retention as it failed to disclose the inadequate security practices previously alleged.

172. If Plaintiff and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to secure their Private Information, they would have made alternative employment choices that excluded Defendant.

173. Plaintiff and Class Members have no adequate remedy at law.

174. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

175. As a direct and proximate result of Belle Tire's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the imminent and substantial risk of actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses

associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Belle Tire's possession and is subject to further unauthorized disclosures so long as Belle Tire fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

176. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Belle Tire and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Belle Tire from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

177. Plaintiff and Class Members may not have an adequate remedy at law against Belle Tire, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT VI
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFF AND THE NATIONWIDE CLASS)

178. Plaintiff restates and realleges allegations stated from the preceding paragraphs as if fully set forth herein.

179. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and common law described in this Complaint.

180. Belle Tire owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

181. Belle Tire still possesses Private Information regarding Plaintiff and Class Members.

182. Plaintiff alleges that Belle Tire's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his Private Information and the risk remains that further compromises of his Private Information will occur in the future.

183. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Belle Tire owes a legal duty to secure its current and former employees' Private Information from unauthorized disclosure and theft;

b. Belle Tire's existing security measures do not comply with its implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect current and former employees' Private Information; and

c. Belle Tire continues to breach this legal duty by failing to employ reasonable measures to secure current and former employees' Private Information.

184. This Court should also issue corresponding prospective injunctive relief requiring Belle Tire to employ adequate security protocols consistent with legal and industry standards to protect current and former employees' Private Information, including the following:

a. Order Belle Tire to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members; and

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Belle Tire must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including

simulated attacks, penetration tests, and audits on Belle Tire's systems on a periodic basis, and ordering Belle Tire to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Belle Tire's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

vii. routinely and continually purging all former employee data that is no longer necessary in order to adequately conduct its business operations; and

viii. meaningfully educating its current and former employees about the threats they face with regard to the security of their Private Information, as well as the steps Belle Tire's current and former employees should take to protect themselves.

185. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Belle Tire. The risk of another such breach is real, immediate, and substantial. If another breach at Belle Tire occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

186. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Belle Tire if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Belle Tire's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Belle Tire has a pre-existing legal obligation to employ such measures.

187. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Belle Tire, thus preventing future injury to Plaintiff and other current and former employees whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Belle Tire to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Belle Tire to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

Dated: November 12, 2024

Respectfully submitted,

By: /s/ E. Powell Miller
E. Powell Miller (P39487)
Emily E. Hughes (P68724)
THE MILLER LAW FIRM, P.C.
950 West University Drive
Rochester, MI 48307
Tel: (248) 841-2200
epm@millerlawpc.com
eeh@millerlawpc.com

Tyler J. Bean
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
tbean@sirillp.com

Attorneys for Plaintiff and the Putative Class